



Homeland
Security

Daily Open Source Infrastructure Report

25 June 2015

Top Stories

- Severe weather June 23 caused 200,000 power outages in New Jersey, 160,000 in Pennsylvania, 22,700 in Delaware and 20,000 in Connecticut. – *NBC News* (See item [1](#))
- A U.S. and Canadian dual-citizen was arrested June 23 on charges surrounding alleged securities fraud and money laundering conspiracies that generated \$300 million in illegal profits. – *Reuters* (See item [9](#))
- German authorities extradited a Turkish suspect to the U.S. June 23 on charges that he allegedly organized a complex bank heist of \$40 million in cash from ATMs in New York and in 23 other countries in February 2013. – *Bloomberg* (See item [13](#))
- The U.S. Office of Personnel Management's director announced in a Congressional hearing June 24 that the estimated cost for recent data breaches targeting the agency could exceed \$19 million. – *Christian Science Monitor* (See item [26](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
 - [Emergency Services](#)
-

Energy Sector

1. *June 24, NBC News* – (National) **Northeast storms knock out power to hundreds of thousands.** Severe weather June 23 caused 200,000 power outages in New Jersey, 160,000 in Pennsylvania, 22,700 in Delaware and 20,000 in Connecticut. The heavy storms also caused a total of 1,000 flight cancellations and 4,000 delays at Boston, New York, Philadelphia and Washington, D.C. airports.
Source: <http://www.nbcnews.com/news/weather/northeast-storms-knock-out-power-hundreds-thousands-ground-flights-n380751>
2. *June 24, Washington Post* – (Maryland) **One dead in Montgomery county as storms sweep across D.C. region.** Severe weather June 23 caused an estimated 100,000 power outages across Virginia, Maryland and suspended Washington D.C. Amtrak service for 2 hours.
Source: http://www.washingtonpost.com/local/severe-storms-approaching-the-district-70-mph-winds-possible/2015/06/23/8da03b28-19f5-11e5-93b7-5eddc056ad8a_story.html
3. *June 23, Warwick Beacon* – (Rhode Island) **27,000 customers lose electricity.** An equipment failure at the Drum Rock substation caused 27,000 Warwick, Rhode Island residents to lose power June 23.
Source : http://warwickonline.com/stories/27000-customers-lose-electricity,103513?category_id=4&content_class=1&town_id=1&sub_type=stories
4. *June 23, Washington Times* – (Wyoming) **Federal judge blocks Obama from implementing draconian fracking rules.** A Federal district court judge temporarily blocked implementation June 23 of a Bureau of Land Management rule governing fracking on leased Federal lands. The judge wants the BLM to explain by July 22 how it developed the rule, which would apply increased regulation to well construction standards, storage of wastewater and disclosure of the chemicals used in the fracking process, and how it considered comments on it from the public.
Source : <http://www.washingtontimes.com/news/2015/jun/23/judge-postpones-obama-administrations-fracking-rul/>

For additional stories, see items [15](#) and [34](#)

[\[Return to top\]](#)

Chemical Industry Sector

Nothing to report

[\[Return to top\]](#)

Nuclear Reactors, Materials, and Waste Sector

5. *June 24, KWMU 90.7 FM St. Louis* – (Missouri) **Army Corps finds more radioactive**

contamination along Coldwater Creek. U.S. Army Corps of Engineers officials reported June 23 that results from over 4,000 samples taken along Coldwater Creek in St. Louis County revealed low levels of radioactive contamination in the creek's floodplain.

Source: <http://news.stlpublicradio.org/post/army-corps-finds-more-radioactive-contamination-along-coldwater-creek>

6. *June 24, Easton Express-Times* – (Pennsylvania) **Pennsylvania nuclear plant updates procedure, training after violation notice.** The U.S. Nuclear Regulatory Commission issued a Federal notice of violation June 22 to Talen Energy Corp., Susquehanna Nuclear LLC's Susquehanna Steam Electric Station in Salem Township, Pennsylvania following a preliminary "white" finding for the plant's timetable to declare an emergency in the event of a primary coolant system leak outside primary containment. Talen officials reported that they addressed the issue with updated procedures and training.

Source: http://www.lehighvalleylive.com/breaking-news/index.ssf/2015/06/pennsylvania_nuclear_plant_upd.html

For another story, see item [34](#)

[\[Return to top\]](#)

Critical Manufacturing Sector

7. *June 24, Associated Press* – (National) **Ford Motor recalls more than 200,000 vans and SUVs over instrument panel and seat belt issue.** Ford Motor Company is recalling 203,500 model year 2014 – 2015 Transit Connect and Escape vehicles in North America due to issues with warning chimes and lights on vehicle instrument panels that may not function when the vehicle is started.

Source: <http://www.startribune.com/ford-motor-recalls-vans-suvs-over-panel-seat-belt-issues/309528991/>

8. *June 24, ConsumerAffairs.com* – (National) **Ford recalls Mustangs with possible fuel tank issue.** Ford Motor Company is recalling 19,095 model year 2015 Mustang 2.3L engine vehicles due to an issue in which prolonged elevated underbody temperatures could cause fuel tank, vapor, and parking brake cable lines to degrade, increasing risks of fuel leaks, fire, and/or loss of parking brake function.

Source: <http://www.consumeraffairs.com/news/ford-recalls-mustangs-with-possible-fuel-tank-issue-062415.html>

For another story, see item [30](#)

[\[Return to top\]](#)

Defense Industrial Base Sector

See item [30](#)

Financial Services Sector

9. *June 23, Reuters* – (National) **U.S.-Canadian man charged for Cynk trades, \$300 mln fraud.** A U.S. and Canadian dual-citizen was arrested June 23 on charges surrounding alleged securities fraud and money laundering conspiracies that generated \$300 million in illegal profits, including a pump-and-dump scheme that inflated the market value of Cynk Technology Corp to over \$6 billion. The U.S. Securities and Exchange Commission filed related civil charges against the suspect.
Source: <http://www.reuters.com/article/2015/06/23/usa-crime-mulholland-fraud-idUSL1N0Z92FI20150623>
10. *June 23, WPLG 10 Miami* – (International) **Suspect dubbed ‘Lucky Bandit’ bank robber arrested.** FBI officials reported that the suspect dubbed the “Lucky Bandit” was arrested June 23 in connection with a robbery of a Wells Fargo bank and an attempted robbery of a Citibank branch in Pembroke Pines in April. The suspect is believed to be connected to 8 bank robberies since October 2014.
Source: <http://www.local10.com/news/serial-bank-robber-arrested/33740676>
11. *June 23, U.S. Securities and Exchange Commission* – (International) **SEC charges unregistered brokers in EB-5 Immigrant Investor Program.** The U.S. Securities and Exchange Commission charged Florida-based Ireco LLC and its Hong Kong-based successor June 23 with allegedly illegally brokering over \$79 million worth of investments by foreigners seeking U.S. residency in the U.S. Citizenship and Immigration Service’s EB-5 Immigrant Investor Program. The firms agreed to be censured and to cease and desist from similar violations in the future.
Source: <http://www.sec.gov/news/pressrelease/2015-127.html>
12. *June 23, Dark Reading* – (International) **Banks targeted by hackers three times more than other sectors.** Raytheon and Websense released findings from a study on their customers revealing that financial services organizations, many of which are U.S. firms, are targeted three times more by cybercriminals than any other industry, and that these attacks are primarily utilizing the Rerdom, Vawtrack, and Geodo malware families, among other findings.
Source: <http://www.darkreading.com/attacks-breaches/banks-targeted-by-hackers-three-times-more-than-other-sectors/d/d-id/1321016>
13. *June 23, Bloomberg* – (International) **Most-wanted cybercriminal extradited to U.S. from Germany.** German authorities extradited a Turkish suspect, who is considered to be one of the world’s most wanted cybercriminals, to the U.S. June 23 on charges that he allegedly organized a complex bank heist of \$40 million in cash from ATMs in New York and in 23 other countries in February 2013. The suspect also reportedly stole \$19 million through 25,700 ATM transactions in 20 countries from 2011 – 2012.
Source: <http://www.bloomberg.com/politics/articles/2015-06-23/turkish-man-accused-in-global-atm-heist-extradited-to-u-s>

14. *June 22, U.S. Attorney's Office, Eastern District of Pennsylvania* – (National) **RICO conspiracy charged in payday lending case.** A Jenkintown, Pennsylvania was charged in an indictment unsealed June 22 with participation in a racketing conspiracy for allegedly operating a payday lending business that violated numerous State usury laws and reaped millions of dollars from illegal fees, and for allegedly helping his sons in a multi-million-dollar telemarketing scam that victimized over 70,000 people nationwide.

Source: <https://www.fbi.gov/philadelphia/press-releases/2015/rico-conspiracy-charged-in-payday-lending-case>

For another story, see item [28](#)

[\[Return to top\]](#)

Transportation Systems Sector

15. *June 23, WFMZ 69 Allentown* – (Pennsylvania) **Downed power lines shut down Route 422 for more than 12 hours.** Route 422 in Douglass Township reopened in both directions after being closed for more than 12 hours June 23 while crews repaired power lines that were brought down by a semi-truck and caused an electricity and phone service outage in the area. Service was restored.

Source: <http://www.wfmz.com/news/news-regional-berks/downed-power-lines-shut-down-route-422-for-more-than-12-hours/33737600>

16. *June 23, Merced Sun-Star* – (California) **CHP investigates fatal crash on Highway 165 north of Los Banos.** Highway 165 was closed at Highway 140 between Hilmar and Lost Banos and later reopened to one-way traffic after being closed for approximately 3 hours June 23, while crews investigated a fatal 2-vehicle crash that involved a semi-truck and a sedan, killing 1 person.

Source: <http://www.mercedsunstar.com/news/article25357432.html>

17. *June 23, KVVU 5 Las Vegas* – (Nevada) **Motorcyclist killed in crash along northbound I-15.** The northbound lanes of Interstate 15 in Las Vegas were shut down June 23 for approximately 3 hours while crews cleared the scene of a fatal motorcycle accident that involved a motorcycle and a vehicle.

Source: <http://www.fox5vegas.com/story/29390350/fatal-crash-shuts-down-northbound-i-15-near-cheyenne>

For additional stories, see items [1](#), [2](#) and [30](#)

[\[Return to top\]](#)

Food and Agriculture Sector

18. *June 23, U.S. Food and Drug Administration* – (National) **Wish-Bone Salad Dressing issues allergy alert on undeclared egg in 24 oz. Wish-Bone Ranch Salad Dressing.**

The U.S. Food and Drug Administration reported June 23 that Pinnacle Foods Group LLC is recalling a limited quantity of its Wish-Bone Ranch Salad Dressing in 24 oz. bottles due to an undeclared egg allergen and misbranding. The products were shipped nationwide.

Source: <http://www.fda.gov/Safety/Recalls/ucm452491.htm>

19. *June 23, U.S. Food and Drug Administration* – (National) **Good Seed Inc. recalls soybean sprouts and mung bean sprouts due to possible health risk.** Good Seed Inc. of Springfield, Virginia is recalling its packages of soybean sprouts and mung bean sprouts due to potential contamination of listeria monocytogenes. The products were shipped to retail stores in Virginia, Maryland, and New Jersey.

Source: <http://www.fda.gov/Safety/Recalls/ucm452444.htm>

20. *June 23, U.S. Food and Drug Administration* – (California) **La Mexicana announces the recall of Spinach Dip for undeclared allergens.** La Mexicana Food Products of Vernon, California is recalling its 14-ounce Spinach Dip due to an undeclared milk allergen June 22. La Mexicana will notify direct customers about the recall.

Source: <http://www.fda.gov/Safety/Recalls/ucm452484.htm>

21. *June 22, U.S. Food and Drug Administration* – (National) **Project 7 issues allergy alert on undeclared milk/dairy ingredients in Sour Caramel Apple Gum.** Project 7, a San Clemente, California establishment, recalled its 0.53 ounce Sour Caramel Apple Gum distributed from August 2014 – June 2015, due to an undeclared milk allergen June 22. The products were distributed nationwide to various in-store and online retailers.

Source: <http://www.fda.gov/Safety/Recalls/ucm452203.htm>

[\[Return to top\]](#)

Water and Wastewater Systems Sector

22. *June 24, WOWK 13 Charleston* – (West Virginia) **Water outage to last at least another 12 hours after water main break in Dunbar.** West Virginia American Water reported June 24 that it will be at least 12 more hours before water is restored to nearly 25,000 customers in Kanawha and Putnam Counties following a June 23 water main break in Dunbar.

Source: <http://www.wowktv.com/story/29391590/wvam-reports-large-water-outage>

For another story, see item [34](#)

[\[Return to top\]](#)

Healthcare and Public Health Sector

23. *June 24, KVUE 24 Austin* – (Texas) **Health Department investigating cyclospora outbreak.** The Austin and Travis County Health and Human Services Department announced June 23 that it is investigating a cyclospora outbreak in response to 15

confirmed and 11 probable new cases of the intestinal illness.

Source: <http://www.kvue.com/story/news/health/2015/06/23/health-department-investigating-cyclospora-outbreak/29175041/>

24. *June 23, KRQE 13 Albuquerque* – (New Mexico) **Department of Health to screen people exposed to man with tuberculosis.** The Department of Health in Curry County announced June 22 they have identified and are contacting approximately 100 people who may have come in contact with a man who recently tested positive for active tuberculosis.

Source: <http://krqe.com/2015/06/22/departement-of-health-to-screen-people-exposed-to-man-with-tuberculosis/>

For another story, see item [33](#)

[\[Return to top\]](#)

Government Facilities Sector

25. *June 23, IDG News Service* – (International) **US visa system coming back online after major outage.** The U.S. Department of State announced June 23 it would again be able to issue visas after a piece of hardware used in biometric processing failed May 26, halting the Consular Consolidated Database system. Officials warned that the updated system is still being tested and may be taken offline again in the future.

Source: http://www.networkworld.com/article/2939614/us-visa-system-coming-back-online-after-major-outage.html#tk.rss_all

26. *June 23, Christian Science Monitor* – (National) **Price tag for OPM breach at least \$19 million.** The U.S. Office of Personnel Management's director announced in a Congressional hearing June 24 the estimated cost for recent data breaches targeting the agency could exceed \$19 million. The cost covers informing victims of the breach as well as credit monitoring services.

Source: <http://www.csmonitor.com/World/Passcode/2015/0623/Price-tag-for-OPM-breach-at-least-19-million>

27. *June 23, Charlotte Observer* – (North Carolina) **Flood damage closes road to Great Smoky Mountains National Park.** Several roads to the Great Smoky Mountains National Park in North Carolina were closed June 23 after flood damage exposed underground electric and phone lines. All electric power and water services to campground and picnic areas were shut off, and park maintenance crews allowed one-lane traffic to escort visitors from the campground.

Source: <http://www.charlotteobserver.com/news/local/article25335868.html>

For another story, see item [33](#)

[\[Return to top\]](#)

Emergency Services Sector

Nothing to report

[\[Return to top\]](#)

Information Technology Sector

28. *June 24, Softpedia* – (International) **Dyre banking malware uses 285 command and control servers.** Security researchers from Symantec released a report revealing that multiple groups are running at least 285 command and control (C&C) servers as well as 44 machines to deliver payloads and execute man-in-the-browser (MitB) attacks. The servers are located primarily in Ukraine and Russia but located worldwide, and are primarily targeting financial organizations in the U.S. and United Kingdom.
Source: <http://news.softpedia.com/news/dyre-banking-malware-uses-285-command-and-control-servers-485119.shtml>
29. *June 24, The Register* – (International) **Feds count Cryptowall cost: \$18 million says FBI.** The FBI reported that the U.S. Internet Crime Complaints Commission (IC3) received 992 complaints associated with the CryptoWall ransomware resulting in U.S. user and business losses of over \$18 million from April 2014 – June 2015.
Source: http://www.theregister.co.uk/2015/06/24/feds_count_cryptowall_cost_18_million_says_fbi/
30. *June 23, Softpedia* – (International) **Flash Player zero-day used by Chinese Cyber-Espionage group.** Security researchers from FireEye discovered that the APT3 advanced threat group is currently exploiting a zero-day Adobe Flash Player heap buffer overflow vulnerability patched by Adobe June 23. The group's latest campaign was dubbed Operation Clandestine Wolf, and they generally target organizations from the aerospace and defense, construction and engineering, technology, telecommunications, and transportation industries.
Source: <http://news.softpedia.com/news/flash-player-zero-day-used-by-chinese-cyber-espionage-group-485077.shtml>
31. *June 23, Softpedia* – (International) **Cheap radio device can steal decryption keys from nearby laptop.** Researchers from Israel created a palm-sized radio device that can capture decryption keys from laptops just a few feet away by intercepting bit patterns in electromagnetic emanations from the targeted machine's central processing unit (CPU). The device can be built for about \$300 from readily available components, and was able to extract decryption keys within seconds.
Source: <http://news.softpedia.com/news/cheap-radio-device-can-steal-decryption-keys-from-nearby-laptop-485065.shtml>
32. *June 23, SC Magazine* – (International) **Targeted attacks rise, cyber attackers spreading through networks, report says.** Vectra Networks released findings from its Post-Intrusion Report of 40 customer and prospect networks revealing that non-linear growth in lateral movement of attacks increased 580 percent from 2014, that reconnaissance detections were up 270 percent, and that overall detections increased 97

percent. Vectra attributed the large uptick in detections partly to the increased accessibility of hacker tools.

Source: <http://www.scmagazine.com/once-in-attackers-spread-out-through-networks-research-shows/article/422382/2/>

33. *June 23, Dark Reading* – (International) **Government, Healthcare particularly lackluster in application security.** Veracode released findings from its State of Software Security Report revealing that government agencies and healthcare organizations performed the worst in industry-specific software security metrics due to issues such as slow rates in addressing identified flaws and cryptographic vulnerabilities from weak algorithms, while all industries struggled with software supply chain issues, among other findings.
Source: <http://www.darkreading.com/application-security/government-healthcare-particularly-lackluster-in-application-security/d/d-id/1321002>

34. *June 23, Threatpost* – (International) **TCP vulnerability haunts Wind River VxWorks embedded OS.** Security researchers at Georgia Tech discovered a transmission control protocol (TCP) prediction vulnerability in Wind River's VxWorks embedded operating system (OS) used in a large number of industrial control system (ICS) products in which an attacker can leverage a predictable TCP initial sequence to spoof or disrupt connections to and from target devices.
Source: <https://threatpost.com/tcp-vulnerability-haunts-wind-river-vxworks-embedded-os/113429>

35. *June 23, Softpedia* – (International) **Adobe fixes Flash Player zero-day exploited in the wild.** Adobe released an emergency update for its Flash Player software addressing a heap buffer overflow vulnerability that is being exploited in the wild in which an attacker could execute arbitrary code and take control of an affected system, possibly funneling in malware via drive-by download attacks.
Source: <http://news.softpedia.com/news/adobe-fixes-flash-player-zero-day-exploited-in-the-wild-485066.shtml>

For additional stories, see items [12](#) and [13](#)

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <http://www.it-isac.org>

[\[Return to top\]](#)

Communications Sector

36. *June 23, Surf City SandPaper* – (New Jersey) **Hours-long Comcast outage due to software issue, now resolved.** Internet, cable, and phone services were restored to

Comcast customers in northern and central New Jersey, June 23 after the system went down due to a software issue that caused an outage for several hours.

Source: <http://thesandpaper.villagesoup.com/p/hours-long-comcast-outage-due-to-software-issue-now-resolved/1366025>

For additional stories, see items [15](#) and [30](#)

[\[Return to top\]](#)

Commercial Facilities Sector

37. *June 24, Charlotte Time Warner Cable News* – (North Carolina) **Two firefighters treated for head-related illness battling Charlotte church fire.** The Charlotte Briar Creek Road Baptist Church in North Carolina, sustained extensive damage after a 3-alarm fire prompted over 75 firefighters to respond and extinguish the flames June 24. Two firefighters sustained minor injuries and the cause of the fire is unknown.
Source: <http://www.twcnews.com/nc/charlotte/news/2015/06/24/two-firefighters-treated-for-heat-related-illness-battling-charlotte-church-fire.html>
38. *June 24, Birmingham Huntsville Times* – (Alabama) **More than 50 firefighters battled apartment blaze off of U.S. 280.** A June 23 fire at Riverside Park Apartments in Birmingham, Alabama, prompted the response of over 50 firefighters and at least 4 agencies to contain the incident. No injuries were reported and an investigation is ongoing to determine the cause of the blaze.
Source: http://www.al.com/news/birmingham/index.ssf/2015/06/more_than_50_firefighters_batt.html
39. *June 24, WTTG 5 Washington, D.C.* – (Maryland) **Lightning strike causes Greenbelt apartment fire; storm causes damage across region.** Officials reported June 24 that dozens of residents at a Greenbelt, Maryland apartment complex were displaced after a lightning struck the complex, started a 2-alarm fire, and damaged 22 units. No injuries were reported and fire crews contained the incident.
Source: <http://www.myfoxdc.com/story/29396338/lightning-strike>
40. *June 24, KPRC 2 Houston* – (Texas) **Woman charged in connection to apartment fire that displaced 20 families.** A Houston Fire Department official reported June 23 that a woman was charged with arson after setting an apartment complex ablaze, damaging 16 units, and displacing 20 families. Officials are further investigating the case.
Source: <http://www.click2houston.com/news/hfd-on-scene-of-apartment-fire-near-greenspoint/33738442>
41. *June 23, WTVT13 Tampa* – (Washington) **Thieves go beneath Everett dental office to steal all the copper piping from crawlspace.** Everett, Washington, police reported June 23 that Silver Lake Dental Arts was the target of the most costly commercial copper theft to date, as robbers stole the copper piping beneath the facility. An

investigation is ongoing to find the culprits and damages total \$90,000 in losses.

Source: <http://q13fox.com/2015/06/23/thieves-go-beneath-everett-dental-office-to-steal-all-the-copper-piping-from-crawlspace/>

42. *June 23, Ottawa Daily Times; Associated Press* – (Michigan) **Five injured at Lee County camping resort.** Lee County officials reported June 23 that an EF-2 tornado caused extensive damage to Woodhaven Association, a Michigan private camping resort, which injured 5 people and left several trailer homes destroyed. Lee County was declared a disaster area and crews were deployed to find missing families.

Source: http://www.mywebtimes.com/news/local/five-injured-at-lee-county-camping-resort/article_573aa519-a080-55e1-92da-3580b8f6bcb8.html

[\[Return to top\]](#)

Dams Sector

See item [34](#)

[\[Return to top\]](#)



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

Contact Information

Content and Suggestions:

Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590

Subscribe to the Distribution List:

Visit the [DHS Daily Open Source Infrastructure Report](#) and follow instructions to [Get e-mail updates when this information changes](#).

Removal from Distribution List:

Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.